

## Workaround for Deleting User Roles

Currently, security administrators are not able to delete roles from users. This document will describe the steps that can be done to workaround this issue. **It is imperative that the User Security Access Report be pulled in the first step. If this is not done, there is no way to obtain the information after all roles are deleted!**

Below is a summary of the steps that will be performed. Detailed instructions for each step will follow in this document. Note that only someone that is setup as a security administrator in PIC can perform these functions.

- ☐ Step 1: [Generate the User Security Access Report](#) so that you have a record of what roles the user has.
- ☐ Step 2: [Delete all roles](#) from the user.
- ☐ Step 3: [Add the roles](#) that are currently needed back to the user.

### Generate the User Security Access Report

1. From the PIC Main page, single click on the Security Administration sub module link.
2. Single click on the Access Reports tab at the top of the page. The User Security Access report page is the default page displayed.
3. Locate the user in the Security List at the bottom of the page. If you have trouble finding the user, you may need to apply search criteria to narrow down the list. This can be done by:
  - ✓ Single click the User ID or Last Name radio button. Then type all or part of the ID or last name in the Enter Search Text textbox.
  - ✓ You can select the user status – active or inactive – from the Select Status drop down box. If you are unsure or have entered information in the Enter Search Text textbox you can leave this at the default of All.
  - ✓ You do not need to make a selection from the Select ID Type drop down box.
  - ✓ When all criteria have been entered single click the Search button.
4. Once you have located the user ID in the Security List single click on the user ID link to generate the report in a new browser window.
5. Use the printer icon in the upper right corner of the page to print the report. If you have software installed on your computer that allows you to print to a PDF file, you can use this option in the print dialogue box. Once you have printed the report, proceed to the next section of this document.

Security	Role Maint	Access Reports	Activity Reports	User Certification
User Security Access		Privacy Act Access		Global User Search
Select View:		FO HA User		
Field Office HA:		IL003 Peoria Housing Authority		
<b>User Search</b>				
Search for:		User ID <input checked="" type="radio"/> Last Name <input type="radio"/>		
Enter Search Text:		<input type="text"/>		
Select Status:		ALL <input type="button" value="v"/>		
Select ID Type:		ALL <input type="button" value="v"/>		
<input type="button" value="Search"/>				
<b>Security List</b>				
Users 1 to 50 of 51				
User ID▲	User Name▲	User Type▲	ID Type	Status▲
<a href="#">awebb</a>	Andrea Webb	Guest User	User	Inactive

*User Security Access report selection criteria*

## Workaround for Deleting User Roles

User Security Report				
<b>User Identification</b>				
User-id:	MXXXX1		Name (last, first):	User, Bill
Telephone Number:			E-Mail:	bill@domain.gov
User Type:	HA User		User Status:	active
Creation Date :	02/15/2006		Account End Date:	02/15/2007
<b>User Roles</b>				
Module	Sub Module	Role	Level	Entity
PIC Maintenance	User Profile	Use User Profile	FO HA User	User, Bill P
Housing Inventory	Housing Authority	Edit Role	Field Office HA	MD004 MONTGOMERY CO HOUSING AUTHORITY
Housing Inventory	Development	Submit Role	Field Office HA	MD004 MONTGOMERY CO HOUSING AUTHORITY
MTCS	Submission	Submit Role	Field Office HA	MD004 MONTGOMERY CO HOUSING AUTHORITY
MTCS	Viewer	Read Only Privacy	Field Office HA	MD004 MONTGOMERY CO HOUSING AUTHORITY
MTCS	Viewer	Submit Role	Field Office HA	MD004 MONTGOMERY CO HOUSING AUTHORITY
MTCS	Reports	Read Only Privacy	Field Office HA	MD004 MONTGOMERY CO HOUSING AUTHORITY
<b>User Actions</b>				
PIC Maintenance >> User Profile:				
Update User Profile				
Housing Inventory >> Housing Authority:				
Create HA	CreateHAAaddress	CreateHACcontact	ModifyHAAaddress	
ModifyHACcontactAddress	ModifyHACcontactDetails	ModifyHADetails	ModifyOccupancyForm	
Read Development Summary	Read HA Report	Read HA Summary	ReadHAAaddress	
ReadHACcontactAddress	ReadHACcontactDetails	ReadHACcontactList	ReadHADetails	
ReadHAFunding	ReadHAHistoryDetails	ReadHAHistoryList	ReadHAINventory	
ReadHAList	ReadHAPerformance	ReadHAStaffList	ReadHATempOffice	
ReadOccupancyForm	ReadOccupancyReport	ReadSearchHAList		

Example – User Security Access Report

### Delete all roles

Since individual roles cannot be deleted, the workaround is to remove all roles from a user. In the next section you'll be instructed how to add back the roles the user should have.

1. Before proceeding, make sure that you have generated the User Security Access Report in the previous section. If you have not, do so now.
2. In the Security Administration sub module, single click on the user ID for the user you wish to remove the roles from.
3. On the Security Administration Summary page single click on the Remove All Roles link.
4. The page will refresh, and you will see a message that asks you to confirm that you want to remove all assigned roles. Single click on the Remove All Assigned Roles button.

Are you sure you want to remove all roles assigned to this user?

Remove All Assigned Roles

Cancel

**Please note:**

- User profile role will not be removed.
- Existing user roles will be archived prior to removal.
- If you wish to view the roles assigned to the selected user please generate corresponding Security Access Report ("Access Reports" business function tab).

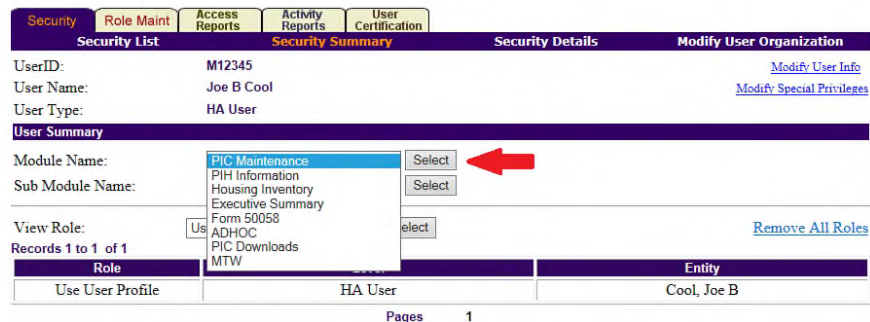
5. The page will refresh, and you will see a message that says, "**All roles assigned to the user: XXXXXX (USER NAME HERE) have been archived and removed (with the exception of User Profile role).**"
6. Once you have removed all roles, proceed to the next section of this document.

## Workaround for Deleting User Roles

### Add roles to use

When you look at the User Security Access Report, you will see all roles that the user had before you deleted them. You will use this report to help you know which roles you need to add back to the user.

1. Before you start to add roles, look at the User Security Access Report to see if there are any sub modules where a user had more than one role for the same entity (e.g. the edit and submit roles for the same PHA code). You will want to make sure you limit each sub module to only one role per entity. *If a user has access to more than one PHA code or field office, it is fine if there are multiple roles as long as there is only one for an entity.*
  - If a user needs access to more than one entity (e.g. PHA, field office, or hub) and the security administrator does not have access to all of those entities, PHAs should contact their local field office PIC Coach. Field offices should follow the protocol for field offices getting assistance with PIC.
2. In the Security Administration sub module, single click on the user ID for the user you wish to add roles to.
3. On the Security Administration Summary page single click on the Module Name drop down box to see the list of modules you can navigate to. Single click on the module name and then single click on the Select button to refresh the page.
  - If you do not see the name of a module you need to assign access to it is because you do not have it and therefore cannot assign access to it. Please consult with another security administrator at your PHA, if there is one, to see if it should be assigned to you or if they can assign that role or contact your local field office PIC coach for assistance.



The screenshot shows the 'Security Administration Summary' page. At the top, there are tabs for 'Security', 'Role Maint', 'Access Reports', 'Activity Reports', and 'User Certification'. Below these, there are sections for 'UserID: M12345', 'User Name: Joe B Cool', and 'User Type: HA User'. A 'Module Name' dropdown menu is open, showing a list of modules including 'PIC Maintenance', 'PIH Information', 'Housing Inventory', 'Executive Summary', 'Form 50058', 'ADHOC', 'PIC Downloads', and 'MTW'. A red arrow points to the 'Select' button next to the dropdown. Below the dropdown, there is a 'View Role' section with a 'Us' button and a 'Records 1 to 1 of 1' indicator. At the bottom, there is a table with columns 'Role' and 'Entity'. The table shows 'Use User Profile' for the role and 'Cool, Joe B' for the entity. The page number '1' is displayed at the bottom.

Role	Entity
Use User Profile	Cool, Joe B

## Workaround for Deleting User Roles

4. Single click on the Sub Module Name drop down box to see the list of sub modules you can navigate to. Single click on the sub module name and then single click on the Select button to refresh the page.
  - If you do not see the name of a sub module you need to assign access to it is because you do not have it and therefore cannot assign access to it. Please consult with another security administrator at your PHA, if there is one, to see if it should be assigned to you or if they can assign that role or contact your local PIC coach for assistance.

The screenshot shows the 'Security Summary' page for user M12345 (Joe B Cool, HA User). The 'Module Name' is 'Form 50058'. The 'Sub Module Name' dropdown is open, showing options: 'Submission' (selected), 'Viewer', 'Reports', and 'Tenant ID Management'. A red arrow points to the dropdown, and another red arrow points to the 'Add Role' link. Below the dropdown is a table with columns: Remove, Role, Level, and Entity. The message 'No Roles Defined.' is displayed below the table.

5. You should see the message “No Roles Defined” underneath the table that would display the details of any roles the user currently has assigned.
6. Single click on the Add Role link. A page similar to the screen print below will appear.

The screenshot shows the 'Role/Data Details' page. The 'Available Roles' dropdown is set to 'Read Only Role'. The 'Security' dropdown is set to 'HQ Office'. A red arrow points to the 'Go' button next to 'Available Roles', another red arrow points to the 'Go' button next to 'Security', and a third red arrow points to the 'View Actions' button. Below these is a table with columns: Field Names and Key Value. The table contains one row: 'HQ Office' and 'Public and Indian Housing'. A red arrow points to the 'Key Value' cell. At the bottom right, there is a 'Save' button highlighted with a red box.

7. On the Add Role page you need to select the role you want to assign. Single click on the Go button to select it. If you are unsure what actions that role will enable the user to perform, you can single click on the View Actions button. If you want to see the actions for a different role you will need to select that role and single click on the Go button to refresh the list. If you click on the View Actions button again it will hide the list of actions after you look at them.

## Workaround for Deleting User Roles

8. Once you have selected the role you will need to select the Security level from the Security drop down box. When you single click on the drop-down box you will see a list of levels. This list may change slightly from one sub module to another. The tips below will help you know what to select. Once you have selected the security level single click the Go button to continue.
  - HA security administrators will typically select “Field Office HA”. For larger PHAs, “Development” may be selected for the Development sub module if a user only needs access to specific developments.
  - HUD security administrators may select “Hub” for all PHAs in that region or “Field Office” for all PHAs under their field office. Do not select “Field Office HA” since this does not work properly for HUD users. *Only security administrators with HQ level security administration access can assign national access.*
9. What you see in the table at the bottom of the page depends on what security level of access the security administrator has and what was select for the security level for the user being worked on. Do not change the HQ Office or HQ Division drop down boxes if they are present. Make the appropriate selections from the hub, field office, and field office HA boxes as necessary. When you make a selection in the hub or field office drop down boxes you will need to use the Go button to cause the page to refresh and show you an updated list of choices. This is where you would select more than one entity if needed. When you are finished, single click the Save button to finish assigning the role to the user.

**Note: In some cases, users are getting a 9605 error message when adding a role. This appears to be an intermittent issue and typically is resolved by logging out, closing your browser, and trying again in 30 minutes. Typically, after this much time you will be logged into a different server.**

The screenshot shows the 'Role Maintenance' web application interface. The 'Security' tab is active, displaying the 'Security Summary' section. The 'Security' dropdown menu is set to 'Field Office HA'. The 'Field Office' dropdown menu is set to 'QAPH SEATTLE HUB OFFICE'. The 'Field Office HA' list contains several options, with 'AK001 AHFC - MTW PH' selected. The 'Save' button is highlighted with a red box.

Field Names	Key Value
HQ Office	Public and Indian Housing
HQ Division	PO Field Operations
Hub	10HSEA Seattle Hub
Field Office	QAPH SEATTLE HUB OFFICE
Field Office HA	AK001 AHFC - MTW PH AK901 AHFC - MTW VO ID001 Twin Falls ID002 Nampa ID005 Pocatello ID007 COEUR D'ALENE TRIBAL HA ID008 NEZ PERCE TRIBAL HA ID009 FORT HALL HA ID010 Buhl ID011 Jerome

☐ Select/Deselect All

**Save**

*Add Role – Security level selection for the selected role*

## Workaround for Deleting User Roles

Security	Role Maint	Access Reports	Activity Reports	User Certification
Security List		Security Summary		Security Details
Modify User Organization				
UserID:	M12345			<a href="#">Modify User Info</a>
User Name:	Joe B Cool			<a href="#">Modify Special Privileges</a>
User Type:	HA User			
<b>User Summary</b>				
Module Name:	Form 50058	▼	Select	
Sub Module Name:	Viewer	▼	Select	
View Role:	Submit EOP Role	▼	Select	<a href="#">Add Role</a> <a href="#">Remove All Roles</a>
Records 1 to 1 of 1				
Remove	Role	Level	Entity	
<input type="checkbox"/>	Submit EOP Role	Field Office HA	CO001 DENVER	
<input type="checkbox"/> Select/DeSelect All				
<a href="#">Remove Role</a>				
Pages 1				

*Security Administration Summary – shows the role just assigned*

10. You will repeat steps 3-9 to assign additional roles to this user. When you have completed your work remember to log out of PIC using the Logoff link and to also log out of Secure Systems.